

## UNITED STATES DISTRICT COURT

for the  
Western District of Washington

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Case No. MJ20-487

INFORMATION ASSOCIATED WITH THREE TARGET  
TELEPHONES, AS DESCRIBED IN  
ATTACHMENT A-1 & A-2

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachments A1 & A-2, which are incorporated herein by reference

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☐ evidence of a crime;  
☐ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☒ a person to be arrested or a person who is unlawfully restrained.

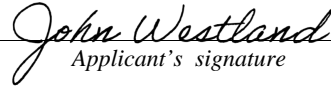
The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
Title 21, USC Section 841(a)(1)	Title 21, USC Section 841(a)(1)

The application is based on these facts:

See the affidavit of US Deputy Marshal John Westland

- ☒ Continued on the attached sheet.  
☒ Delayed notice of 90 days (give exact ending date if more than 30 days: 10/29/2020) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


  
Applicant's signature

John Westland, Deputy U.S. Marshal

Printed name and title

Sworn to before me and signed in my presence.

Date: 07/31/2020

  
Judge's signature

City and state: Seattle, WA

Brian A. Tsuchida, U.S. Magistrate Judge

Printed name and title

# AFFIDAVIT OF JOHN WESTLAND

STATE OF WASHINGTON           )  
                                       )          SS  
COUNTY OF KING              )

I, John Westland, being first duly sworn on oath, depose and say:

## I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Deputy United States Marshal (DUSM) assigned to the Western District of Washington. I began my employment with the United States Marshals Service in 2005. I graduated from the United States Marshals Service Training Academy and the Federal Law Enforcement Training Center for Criminal Investigators. I am currently assigned to the Pacific Northwest Violent Offender Task Force in the Western District of Washington. One of my responsibilities is to locate and apprehend fugitives, to bring them before the court for their charged crimes.

2. During my employment with the United States Marshals Service I have interviewed hundreds of associates, witnesses, and suspects. I am familiar with the manner in which crimes are committed and how suspects attempt to avoid prosecution/apprehension. I have conducted and been a part of numerous surveillances and have authored and served many Pen Register and Trap and Trace Device Orders, Tracking Warrants, Search Warrants, and Arrest Warrants.

## II. PURPOSE OF THIS AFFIDAVIT

3. I make this affidavit in support of an application for: (1) search warrant for historical cell site data, (2) cell site simulator warrants, and (3) tracking warrants for cellular telephones. Separately, the government is also seeking Pen Register Trap and Trace Orders.

4. All of these applications are for three cellular devices (the **Target Telephones**), described as follows:



1 and CR20-094 RSM. ALVAREZ, SUAREZ, and GALINDO are the subjects of an  
 2 ongoing Drug Enforcement Administration (DEA) criminal investigation for knowingly  
 3 and intentionally conspiring to distribute substances controlled under Title 21, United  
 4 States Code, Section 821, Schedules I and II, including cocaine, heroin, and  
 5 methamphetamine, contrary to the provisions of Title 21, United States Code, Sections  
 6 841(a)(1).

7 8. Law enforcement has been unable to locate ALVAREZ, SUAREZ, and  
 8 GALINDO with precision through public information, use of informants, law  
 9 enforcement databases, or traditional surveillance methods.

10 9. On July 24, 2020, the Drug enforcement Administration delegated primary  
 11 apprehension authority to the United States Marshals Service.

12 10. I have learned from Investigators with the DEA that, based on DEA's  
 13 investigation in this matter:

14 a. ALVAREZ has a cellular telephone with AT&T Communications  
 15 number (425) 283-2081 (**Target Telephone A**); when this number is run through a law  
 16 enforcement database, it shows the subscriber as "Wireless Caller."

17 b. SUAREZ has a cellular telephone with AT&T Communications  
 18 number (206) 599-9327 (**Target Telephone B**); when this number is run through a law  
 19 enforcement database, it shows the subscriber as "Sosa Martin."

20 c. GALINDO had a cellular telephone with T-Mobile number (360)  
 21 854-1592 (**Target Telephone C**). Additionally, when this number is run through a law  
 22 enforcement database, it shows the subscriber as "MEJIA FER."

#### 23 IV. MANNER OF EXECUTION

##### 24 A. Historical Cell Site Data.

25 11. In my training and experience, I have learned that AT&T Communications,  
 26 LLC, is a company that provides cellular telephone access to the general public. I also  
 27 know that providers of cellular telephone service have technical capabilities that allow  
 28 them to collect and generate information about the locations of the cellular telephones to

1 which they provide service, including cell-site data, also known as “tower/face  
2 information” or “cell tower/sector records.” Cell-site data identifies the “cell towers”  
3 (i.e., antenna towers covering specific geographic areas) that received a radio signal from  
4 the cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which  
5 the telephone connected. These towers are often a half-mile or more apart, even in urban  
6 areas, and can be 10 or more miles apart in rural areas. Furthermore, the tower closest to  
7 a wireless device does not necessarily serve every call made to or from that device.  
8 Accordingly, cell-site data provides an approximate location of the cellular telephone but  
9 is typically less precise than other types of location information, such as E-911 Phase II  
10 data or Global Positioning Device (“GPS”) data.

11 12. Based on my training and experience, I know that AT&T Communications,  
12 LLC, and T-Mobile can collect cell-site data about the Target Telephones. I also know  
13 that wireless providers such as AT&T and T-Mobile typically collect and retain cell-site  
14 data pertaining to cellular phones to which they provide service in their normal course of  
15 business in order to use this information for various business-related purposes.

16 13. Only some providers are capable of providing latitude-longitude data  
17 (sometimes referred to as “E-911 data” or “GPS data”) at all; most of those providers do  
18 not retrieve or store this kind of data in the normal course of business but must instead  
19 undertake additional steps to generate the data in response to a law enforcement request.

20 14. Some providers also collect per-call measurement data, referred to as the  
21 “real-time tool” (“RTT”). RTT data estimates the approximate distance of the cellular  
22 device from a cellular tower based on the speed with which signals travel between the  
23 device and the tower. This information can be used to estimate an approximate location  
24 range that is more precise than typical cell-site data.

25 15. Based on my training and experience, I know that wireless providers such  
26 as AT&T and T-Mobile typically collect and retain information about their subscribers in  
27 their normal course of business. This information can include basic personal information  
28 about the subscriber, such as name and address, and the method(s) of payment (such as

1 credit card account number) provided by the subscriber to pay for wireless telephone  
2 service. I also know that wireless providers such as AT&T and T-Mobile typically collect  
3 and retain information about their subscribers' use of the wireless service, such as records  
4 about calls or other communications sent or received by a particular phone and other  
5 transactional records, in their normal course of business. In my training and experience,  
6 this information may constitute evidence of the crimes under investigation because the  
7 information can be used to identify the Target Telephones' user or users and may assist in  
8 the identification of co-conspirators and/or victims.

9 **B. Cell Site Simulator.**

10 16. In my training and experience, I have learned that cellular phones and other  
11 cellular devices communicate wirelessly across a network of cellular infrastructure,  
12 including towers that route and connect individual communications. When sending or  
13 receiving a communication, a cellular device broadcasts certain signals to the cellular  
14 tower that is routing its communication. These signals include a cellular device's unique  
15 identifiers.

16 17. To facilitate execution of this warrant, law enforcement may use an  
17 investigative device or devices capable of broadcasting signals that will be received by  
18 the Target Telephones or receiving signals from nearby cellular devices, including the  
19 Target Telephones. Such a device may function in some respects like a cellular tower,  
20 except that it will not be connected to the cellular network and cannot be used by a cell  
21 phone to communicate with others. The device may send a signal to the Target  
22 Telephones and thereby prompt it to send signals that include the unique identifier of the  
23 device. Law enforcement may monitor the signals broadcast by the Target Telephones  
24 and use that information to determine the Target Telephones' location, even if located  
25 inside a house, apartment, or other building.

26 18. The investigative device may interrupt cellular service of phones or other  
27 cellular devices within its immediate vicinity. Any service disruption to non-target  
28 devices will be brief and temporary, and all operations will attempt to limit the

1 interference with such devices. In order to connect with the Target Telephones, the  
2 device may briefly exchange signals with all phones or other cellular devices in its  
3 vicinity. These signals may include cell phone identifiers. The device will not complete  
4 a connection with cellular devices determined not to be the Target Telephones, and law  
5 enforcement will limit collection of information from devices other than the Target  
6 Telephones.

7 19. Investigators intend to use the cell site simulator (CSS) in the vicinity of the  
8 Target Telephones according to prospective cell site location information (CSLI) that is  
9 being provided by AT&T and T-Mobile with the court-ordered intercept. A cell-site  
10 simulator is a mobile device that law-enforcement agents can use to locate a cell phone  
11 whose identifiers are already known to law enforcement and surgically targets the  
12 fugitive's device only. The USMS intends to apprehend ALVAREZ, SUAREZ, and  
13 GALINDO by establishing traditional surveillance in the more precise location derived  
14 from use of the CSS and CSLI data from AT&T and T-Mobile and place the subjects in  
15 custody on the authority of the arrest warrants.

16 20. To the extent that any information from a cellular device other than the  
17 Target Telephones are collected by the law enforcement device, law enforcement will  
18 delete that information, and law enforcement will make no investigative use of it absent  
19 further order of the court, other than distinguishing the Target Telephones from all other  
20 cellular devices.

21 21. As further specified in Attachment B, which is incorporated into the  
22 warrant, the proposed search warrant does not authorize the seizure of any tangible  
23 property. Moreover, to the extent that the warrant authorizes the seizure of any wire or  
24 electronic communication (as defined in 18 U.S.C. § 2510) or any stored wire or  
25 electronic information, there is reasonable necessity for the seizure for the reasons set  
26 forth above. 18 U.S.C. § 3103a(b)(2).  
27  
28



1 **C. Tracking Warrants.**

2 22. In my training and experience, I have learned that AT&T and T-Mobile are  
3 companies that provides cellular telephone access to the general public. I also know that  
4 providers of cellular telephone service have technical capabilities that allow them to  
5 collect and generate at least two kinds of information about the locations of the cellular  
6 telephones to which they provide service: (1) E-911 Phase II data, also known as GPS  
7 data or latitude-longitude data; and (2) cell-site data, also known as “tower/face  
8 information” or cell tower/sector records. E-911 Phase II data provides relatively precise  
9 location information about the cellular telephone itself, either via GPS tracking  
10 technology built into the phone or by triangulating on the device’s signal using data from  
11 several of the provider’s cell towers. Cell-site data identifies the “cell towers” (i.e.,  
12 antenna towers covering specific geographic areas) that received a radio signal from the  
13 cellular telephone and, in some cases, the “sector” (i.e., faces of the towers) to which the  
14 telephone connected. These towers are often a half-mile or more apart, even in urban  
15 areas, and can be ten or more miles apart in rural areas. Furthermore, the tower closest to  
16 a wireless device does not necessarily serve every call made to or from that device.  
17 Accordingly, cell-site data is typically less precise than E-911 Phase II data.

18 23. Based on my training and experience, I know that AT&T and T-Mobile can  
19 collect E-911 Phase II data about the location of the Target Telephones, including by  
20 initiating a signal to determine the location of the Target Telephones on AT&T’s or T-  
21 Mobile’s network or with such other reference points as may be reasonably available.

22 24. Based on my training and experience, I know that AT&T and T-Mobile can  
23 collect cell-site data about the Target Telephones.

24 25. In my experience, cell-site data and GPS location tracking data is useful in  
25 corroborating movements of individuals. Specifically, in this case, historical cell-site data  
26 and real-time GPS location tracking data would provide critical information that would  
27 assist in law enforcement’s effort to locate and arrest ALVAREZ, SUAREZ, and  
28 GALINDO.



## V. AUTHORIZATION REQUEST

26. Based on the foregoing, I request that the Court issue: (1) search warrants for historical cell site data, (2) cell site simulator warrants, and (3) tracking warrants for cellular telephones, pursuant to 18 U.S.C. § 2703(c)(1)(A) and Federal Rule of Criminal Procedure 41.

27. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrants to delay notice until 90 days after the collection authorized by the warrants have been completed. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrants may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the person carrying the Target Telephones would seriously jeopardize the ongoing investigation, as such as a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). There is reasonable necessity for the use of the technique described above, for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2).

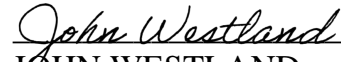
28. I further request that the Court authorize execution of the warrants at any time of the day or night, owing to the potential need to locate the Target Telephones outside of daytime hours.

29. I further request that the Court order that all papers in support of this application, including the affidavit, order, and warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all the targets of this investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize the investigation.

## VI. CONCLUSION

Based upon the foregoing facts and my knowledge of this investigation, I respectfully submit that Rodrigo ALVAREZ-Quinonez, Saul SUAREZ-Mata, and

1 Wilmer GALINDO-Maradiaga are using the Target Telephones and are federal fugitives.  
2 I believe that authorizations sought through this application will assist in locating the  
3 Target Telephones and ALVAREZ, SUAREZ, and GALINDO.  
4

5   
6 JOHN WESTLAND  
7 Deputy US Marshal  
8 United States Marshals Service  
9

10 The above-named agent provided a sworn statement to the truth of the foregoing  
11 affidavit by telephone on 31st day of July, 2020.  
12

13   
14 BRIAN A. TSUCHIDA  
15 United States Magistrate Judge  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**Attachment A-1**  
**Property to be Searched**

This warrant authorizes the use of the electronic investigative technique described in Attachment B to gather information about and identify the location of the following cellular telephones:

1. **Target Telephone A** - assigned call number (425) 283-2081, whose wireless service provider is a company headquartered at 208 S. Akard Street, Suite 2954, Dallas, Texas 75202 (hereafter “**AT&T**”).
2. **Target Telephone B** - assigned call number (206) 599-9327, whose wireless service provider is a company headquartered at 208 S. Akard Street, Suite 2954, Dallas, Texas 75202 (hereafter “**AT&T**”).

This warrant authorizes disclosure of information, as described in Attachment B, about the location of the Target Telephone(s) described above that is within the possession, custody, or control of **AT&T**, including information about the location of the cellular telephone not only as applied to the above assigned call number but as to (i) any instrument to which the listed target telephone number was assigned within the last 30 days, and that now has been assigned a changed telephone number, (ii) any changed telephone number(s) assigned to an instrument now bearing the same ESN/IMSI/IMEI as the telephone number listed above, or that was bearing the same ESN/IMSI/IMEI as the telephone number listed above, at any point within the last 30 days, (iii) any changed ESN subsequently assigned to the same telephone numbers, or (iv) any additional changed telephone number(s) and/or ESN/IMSI/IMEI, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the telephone number listed above, within the period of disclosure authorized by the order.

**AT&T** is referred to in Attachment B as the “Wireless Provider” or “Provider.”

**Attachment A-2**  
**Property to be Searched**

This warrant authorizes the use of the electronic investigative technique described in Attachment B to gather information about and identify the location of the following cellular telephones:

1. **Target Telephone C** - assigned call number (360-854-1592), whose wireless service provider is T-Mobile US, Inc. a company headquartered at 4 Sylvan Way, Parsippany, NJ, 07054 (hereafter “**T-Mobile**”).

This warrant authorizes disclosure of information, as described in Attachment B, about the location of the Target Telephone(s) described above that is within the possession, custody, or control of **T-Mobile**, including information about the location of the cellular telephone not only as applied to the above assigned call number but as to (i) any instrument to which the listed target telephone number was assigned within the last 30 days, and that now has been assigned a changed telephone number, (ii) any changed telephone number(s) assigned to an instrument now bearing the same ESN/IMSI/IMEI as the telephone number listed above, or that was bearing the same ESN/IMSI/IMEI as the telephone number listed above, at any point within the last 30 days, (iii) any changed ESN subsequently assigned to the same telephone numbers, or (iv) any additional changed telephone number(s) and/or ESN/IMSI/IMEI, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the telephone number listed above, within the period of disclosure authorized by the order.

**T-Mobile** is referred to in Attachment B at the “Wireless Provider” or “Provider.”

**ATTACHMENT B****ITEMS TO BE SEIZED****I. Information to be Disclosed by the Wireless Provider**

To the extent that the information described in Attachment A-1 and A-2 is within the possession, custody, or control of the Provider, including any information that has been deleted but is still available to the Provider or that has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose to the government the following information pertaining to the Account listed in Attachment A for the time period July 31, 2020, through September 29, 2020:

- a. The following information about the customers or subscribers of the Account:
  - i. Names (including subscriber names, user names, and screen names);
  - ii. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
  - iii. Local and long distance telephone connection records;
  - iv. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol (“IP”) addresses) associated with those sessions;
  - v. Length of service (including start date) and types of service utilized;
  - vi. Telephone or instrument numbers (including MAC addresses, Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifier (“MEID”); Mobile Identification Number (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”); International Mobile Subscriber Identity Identifiers (“IMSI”), or International Mobile Equipment Identities (“IMEI”);
  - vii. Other subscriber numbers or identities (including the registration Internet Protocol (“IP”) address); and
  - viii. Means and source of payment for such service (including any credit card or bank account number) and billing records.
- b. All records and other information (not including the contents of communications) relating to wire and electronic communications sent or received by the Account, including:
  - i. the date and time of the communication, the method of the communication, and the source and destination of the communication (such as the source and destination telephone numbers (call detail records), email addresses, and IP addresses); and
  - ii. information regarding the cell tower and antenna face (also known as “sectors”) through which the communications were sent and received as well as per-call measurement data (also known as the “real-time tool” or “RTT” data), if available.

**II. Information to be Seized by the Government**

All information described above in Section I that identifies (a) Rodrigo ALVAREZ-Quinonez, (b) Saul SUAREZ-Mata; and/or (c) Wilmer GALINDO-Maradiaga, their residences, employment, or habitual locations during the time period of July 31, 2020, through September 29, 2020, that may facilitate their arrests for violations of Title 21, United States Code, Section 841(a)(1).